SPECIFICATION

Please amend the paragraph beginning on page 4, line 25, as follows:

Certificates often contain additional information that identifies an individual as a member of a particular organization and perhaps the role that they play in the organization. For example, the certificate may ~~identifying~~identify the certificate holder as being an employee of a company or a customer or subcontractor or supplier of the company. The policies determining who is eligible to hold a certificate are therefore important if individuals and organizations are to rely upon this information. These policies govern the overall operation of the certificate authority.

Please amend the paragraph beginning on page 5, line 10, as follows:

The policies under which users register for certificates determine the initial degree of trust that a relying party should place in a certificate. However, the manner in which the public key associated with the certificate is protected is equally as important. Private keys may be stored in any of several different ways. They may be placed on password protected public storage media, such as directories or databases. They may also be stored on password protected media accessible only to the certificate holder or to a relatively small number of persons, such as a floppy disk, the hard drive of the certificate holder's personal computer, or a portable storage device such as a smart card. A more secure storage medium is provided by hardware tokens containing encryption "engines." These hardware tokens actually generate and store the private key and perform all encryption/decryption functions within the token. Hardware tokens typically require a password to activate and, since they remain in the ~~position~~possession of the certificate holder at all times, are substantially more secure than other storage media.

Please amend the paragraph beginning on page 9, line 26, as follows:

Fig. 1 illustrates an exemplary architecture of a network 100 in which the Public Key Infrastructure (P.K.I.) processes of the present invention may be practiced. However, it should be understood that the present invention is not limited to the network 100 of ~~FIG~~Fig. 1. The network 100 includes data entry 102, which performs a data entry function for authoritative

database 104, which is resident on the server platform 106. A server platform 106 is referred to in this description, but it should be understood that the present invention is not limited to any particular server architecture. The server platform 106 may be, without limitation, a ~~UNIX~~UNIX® or ~~Windows NT~~WINDOWS NT® server. The authoritative database 104 contains information about members of the group or enterprise for which PKI services in accordance with the present invention are performed. The present invention is not limited by the structure of the group enterprise for which information is stored in the authoritative database 104. The authoritative database 104 information includes, without limitation, the name, address, telephone numbers, manager's name, employee identification, etc., of the members of the group or enterprise. Directory 108 has the structure of the database but is optimized for fast look-up of information stored therein rather than fast data entry. The data in the directory 108 is not changed frequently but is required to be accessed rapidly and functions on-line as a fast phone book, containing reference information in the authoritative database 104. Certificate authority 110 is off-the-shelf software executed on server platform 106, providing storage of certificates and related information used by the present invention as described in more detail hereinafter. Registration authority 112 is also off-the-shelf software executable on server platform 106 regarding registration performed by the present invention as described in more detail hereinafter. Key authority 114 is also off-the-shelf server software which is executable on server platform 106 for recovering keys from members of the group or enterprise as described in more detail hereinafter. ~~Windows 2000~~WINDOWS 2000® Domain CA 116 may use certificates provided by the present invention for a single sign-on to the network 100 of ~~FIG~~Fig. 1. Legacy server 118 executes legacy application programs 120. The legacy server may be, without limitation, a main frame, mini-computer, workstation, or other server hosting legacy software applications that are designed to be run on PKI processes in accordance with the present invention. The legacy applications 120 are accessible on the client side by a custom client 128 such as an emulator or custom database Graphic User Interface (GUI). Examples of emulators are terminal emulators of an ~~IBM~~IBM® 3270 or terminal emulators of a [[vt]]VT 100. Registration web page 122, which may be one or more pages, functions as the user interface to the network 100 of Fig. 1. Web

server 124 is a software application which serves Web Pages, such as Web Page 122 or other HTML outputs, to a web browser client which may be, without limitation, ~~Apache~~APACHE® or ~~Microsoft~~MICROSOFT® Internet Information Server. Web browser 126 is resident on client platform 128 which may be any user computer. Web browser 126 is a client software application for browsing web pages such as but not limited to, HTML or XML protocols or other protocols. The Web browser 126 is programmed to operate with PKI certificates issued by the certificate authority 110. Examples of web browsers which have this capability are ~~Netscape Navigator~~NETSCAPE NAVIGATOR® and the ~~Microsoft Internet Explorer~~MICROSOFT INTERNET EXPLORER®. The token 130 is a smart card, USB (United Serial Bus), or other hardware token capable of generating, storing, and using PKI certificates. A user 132 is a person using the network 100. A user 132 transitions though a number of states which include a new user, current user, and a former user who no longer is a member of the group or enterprise. The network 100 is described with reference to two levels of security, but the number of the levels of security is not a limitation of the present invention, with each level corresponding to a different security requirement. The level 1 search engine 134 is a search engine which is permitted to search through the network 100 but is allowed access to only level 1 data, which is the lowest level of security and may be, without limitation, data which is freely distributable. Level 2 data may be considered to be proprietary. Level 2 search engine 136 is a search engine which is allowed to search through both level 1 and level 2 data. A level N search engine (not illustrated) is a search engine which is allowed to search through servers possessing data levels 1 through N. A secured level server with level 1 data 138 is a Web server containing only level 1 data, which is secured so that users must have level 1 access (at least) to access the server. A secured Web server with level 2 data 140 is a Web server that contains level 2 data which has been secured so that users must have level 2 access, with level 2 users having access to both level 1 and level 2 servers. A secured Web server with level N data (not illustrated) is a Web server that contains level N data which is accessible by a user with level N or above access. VPN Extranet 142 is a software application which functions as a network gateway which, is illustrated, may be either to legacy server 118 and legacy application 120 or to an external network such as the Internet.

Personal revocation authority 144 is a person who is in charge of revocation of members from the network 100. Personal registration authority 146 is a person who is in charge of registration of members in the network 100. Personal recovery approval 148 is a person in charge of obtaining recovery of certificates. A Recovery Agent 150 is a person who performs recovery of certificates and may only recover a certificate if the certificate has first been designated as recoverable by another person. Personal role approval 152 is a person who approves different role functions within the network 100. A Web server administrator 154 is in charge of various web functions in the network 100.

Please amend the paragraph beginning on page 16, line 18, as follows:

In step 9, the personal registration authority 146 delivers registration information to the new user 132 in a face-to-face meeting. In step 10a, the new user 132 revisits the special registration Web page 350 and can forward the requisite registration information. The special registration of the Web page 350 can only be accessed by using a hardware token 130 that has been pre-loaded with the requisite role certificate and associated private key (from step 0a). In step 11a, the registration Web server 124 signals the registration authority 112 to register the new user 132 possessing the hardware token 130 and in step 12a, the registration authority 112 signals the client platform 128 to generate a private/public key pair on the hardware token 130. Before the public key is sent to the certificate authority, the token can sign the certificate request before the certificate leaves the token, using the private key. This allows the certification authority to know that the pedigree is valid for the highest level of assurance in the reliability of the key storage mechanism. In step 13, the public key is sent from the client platform 128 to the certificate authority 110, which records the certificate pedigree as a certificate policy object identifier (OID) in the certificate itself. Before signing the certificate, the certification authority validates that the certificate request was signed by the token itself. This makes any Trojan horse attack impossible because only a valid token, with the valid private key for a specific pedigree could have signed the request. In step 14, the certificate authority 110 sends the signed certificate (with public key) to the directory 108. In step 15a, the registration Web server 124

alerts the directory 108 that this certificate was generated on the hardware token 130. The Web server 124 knows this because of the fact that only a user [[130]]132 having a hardware token 130 would have been able to access the special version of the registration Web page 350.

Please amend the paragraph beginning on page 19, line 15, as follows:

An advantage of the present invention is that it allows existing commercial products and network standards to accomplish a new kind of functionality, that is, the automated tracking of the pedigree of an individual certificate. As a consequence thereof, PKI systems that are highly automated can now enjoy a feature that was previously only available with manually intensive PKI systems. Thus, the use of this invention yields a significant cost saving when applied to both existing and future PKI system architectures.